REMARKS

By this Amendment, Applicants amend the title of the specification according to the Examiner's suggestion. Applicants also amend claims 2-6, 9-12, and 17-19. Claims 2-19 are currently pending.

In the Office Action, the Examiner allowed claim 19. The Examiner maintained the objection of claim 16, but indicated that claim 16 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The Examiner rejected claim 11 under 35 U.S.C. § 112, second paragraph, as indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner also rejected claims 2-4, 6, 7, and 9 under 35 U.S.C. § 102(e) as anticipated U.S. Patent No. 6,397,241 to Glaser et al. (hereinafter "Glaser"); rejected claims 11, 17, and 18 under 35 U.S.C. § 102(e) as anticipated U.S. Patent No. 6,230,179 to Dworkin et al. (hereinafter "Dworkin"); rejected claims 5 and 10 under 35 U.S.C. § 103(a) as unpatentable over Glaser; rejected claim 8 under 35 U.S.C. § 103(a) as unpatentable over Glaser in view of Becker, 4-bit Multiplier using Mentor Graphics, Student Lab-Report for Course BEng 2, University of East London (August 12, 1998) (hereinafter "Becker"); rejected claim 12 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of U.S. Patent No. 4,692,888 to New (hereinafter "New"); rejected claim 13 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of New, and further in view of U.S. Patent No. 3,064,896 to Carroll et al. (hereinafter "Carroll"); and rejected claims 14 and 15 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of New and Carroll, and further in view of U.S. Patent No. 5,468,297 to Zook (hereinafter "Zook").

Applicants thank the Examiner for allowing claim 19 and pointing out allowable subject matter in claim 16. However, Applicants respectfully traverse the Examiner's rejections under 35 U.S.C. § 102, 103, and 112.

Regarding the Rejections Under 35 U.S.C. § 112

Applicants have amended claim 11 to clarify that "the processing of modular multiplication" is divided into "polynomial multiply processing and a modulo." Accordingly, Applicants respectfully request withdrawal of the rejection of claim 11.

Regarding the Rejections Under 35 U.S.C. § 102

Applicants respectfully traverse the Examiner's rejection of claims 2-4, 6, 7, and 9 under 35 U.S.C. § 102(e) as anticipated by Glaser. In order to anticipate Applicants' claimed invention under 35 U.S.C. § 102, each and every element of the claim in issue must be found, either expressly described or under principles of inherency, in a single prior art reference. Further, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claim." See M.P.E.P. § 2131, quoting Richardson v. Suzuki Motor Co., 868 F.2d 1126, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989), emphasis added.

Claim 2, as amended, recites a combination including, for example, "an arithmetic unit comprising: an integer based unit arithmetic circuit; a finite field GF(2^m) based unit arithmetic circuit logically adjacent to said integer based unit arithmetic circuit; and a selector configured to select one of said integer unit arithmetic circuit and said finite field GF(2^m) based unit arithmetic circuit, and a controller controlling said selector to make said selection." Glaser fails to disclose the elements recited in amended claim 2, as quoted above.

Glaser teaches "an integrated cryptographic system 10 having an RSA arithmetic processor 18 and a separate ECC arithmetic processor 20." Glaser, FIG. 1, column 2, lines 10-15. "A control circuit 16 provides control signals that manage the transfer of data values between memory 14, RSA arithmetic processor 18, ECC arithmetic processor 20." Glaser, FIG. 1, column 3, lines 3-6. However, Glaser's teaching of the "integrated cryptographic system" does not constitute a teaching of "an arithmetic unit comprising: an integer based unit arithmetic circuit; a finite field GF(2^m) based unit arithmetic circuit logically adjacent to said integer based unit arithmetic circuit; and a selector configured to select one of said integer unit arithmetic circuit and said finite field GF(2^m) based unit arithmetic circuit, and a controller controlling said selector to make said selection," as required by amended claim 2. (emphasis added).

Therefore, Glaser fails to disclose each and every element of Applicants' invention recited in amended claim 2, either expressly or inherently. Thus, Glaser cannot anticipate claim 2 under 35 U.S.C. § 102(e). Accordingly, Applicants respectfully request withdrawal of the rejection of claim 2. Since claims 3 and 4 depend on claim 2, Applicants also request withdrawal of the rejection of claims 3 and 4 for at least the same reasons stated above.

Claim 6, as amended, recites a combination including, for example, "a controller configured to output, to said integer unit arithmetic circuit, a selection signal for selecting one of an integer unit arithmetic operation and finite field GF(2^m) based unit arithmetic operation." Glaser fails to disclose at least "a controller configured to output, to said integer unit arithmetic circuit, a selection signal for selecting one of an integer unit

arithmetic operation and finite field GF(2^m) based unit arithmetic operation," as required by amended claim 6.

As explained above, Glaser teaches "an integrated cryptographic system 10 having an RSA arithmetic processor 18 and a separate ECC arithmetic processor 20." Glaser, FIG. 1, column 2, lines 10-15, emphasis added. "A control circuit 16 provides control signals that manage the transfer of data values between memory 14, RSA arithmetic processor 18, ECC arithmetic processor 20." Glaser, FIG. 1, column 3, lines 3-6, emphasis added. Therefore, in Glaser, two separate unit arithmetic circuits perform independent operations while the control circuit coordinates data transfers. Glaser thus does not teach "a controller configured to output, to said integer unit arithmetic circuit, a selection signal for selecting one of an integer unit arithmetic operation and finite field GF(2^m) based unit arithmetic operation," as required by amended claim 6. (emphasis added).

Therefore, Glaser fails to disclose each and every element of Applicants' invention recited in amended claim 6, either expressly or inherently. Thus, Glaser cannot anticipate claim 6 under 35 U.S.C. § 102(e). Accordingly, Applicants respectfully request withdrawal of the rejection of claim 6. Since claims 7 and 9 depend on claim 6, Applicants also request withdrawal of the rejection of claims 7 and 9 for at least the same reasons stated above.

Applicants also respectfully traverse the Examiner's rejection of claims 11, 17, and 18 under 35 U.S.C. § 102(e) as anticipated by Dworkin. Claim 11, as amended, recites a combination including, for example, "an arithmetic unit module including a long product-sum operation circuit which executes only polynomial multiplication with a finite

field GF(2^m) based polynomial base expression." Dworkin fails to disclose at least "an arithmetic unit module including a long product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression," as recited in amended claim 11.

Dworkin teaches an "ALU 4 for implementing multiplication in a finite field," Dworkin, column 4, lines 58-67, and "a controller module/controller (Fig. 1, #20) configured to divide the modular multiplication into multiply processing and a modulo (col. 5, lines 1-10)." (Office Action, at 6). However, the ALU does not constitute ""an arithmetic unit module including a long product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression," as recited in amended claim 11. (emphasis added).

Therefore, Dworkin fails to disclose each and every element of Applicants' invention recited in amended claim 11, either expressly or inherently. Thus, Dworkin cannot anticipate claim 11 under 35 U.S.C. § 102(e). Accordingly, Applicants respectfully request withdrawal of the rejection of claim 11. Since claims 17 and 18 depend on claim 11, Applicants also request withdrawal of the rejection of claims 17 and 18 for at least the same reasons stated above.

Regarding the Rejections Under 35 U.S.C. § 103

Applicants respectfully traverse the Examiner's rejection of claims 5 and 10 under 35 U.S.C. § 103(a) as unpatentable over Glaser. In order to establish a prima facie case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim elements. Second, there must be some suggestion or motivation, either in the references themselves or in

the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Third, there must be a reasonable expectation of success. See M.P.E.P. § 2143.

As explained above, Glaser fails to teach or suggest all elements of Applicants' invention recited in amended claims 2 and 6. Since claims 5 and 10 depend on claims 2 and 6, Applicants respectfully request withdrawal of the rejection of claims 5 and 10 for at least the same reasons stated above in regard to claims 2 and 6.

Applicants also respectfully traverse the Examiner's rejection of claim 8 (dependent from claim 6) under 35 U.S.C. § 103(a) as unpatentable over Glaser in view of Becker. As explained above, Glaser fails to teach or suggest at least "a controller configured to output, to said integer unit arithmetic circuit, a selection signal for selecting one of an integer unit arithmetic operation and finite field GF(2^m) based unit arithmetic operation," as required by amended claim 6.

Becker fails to cure Glaser's deficiencies. Becker teaches "a 4-Bit Multiplier using previous created half- and full-adders," and "[a] 4-Bit multiplier can be realized by using at least 8 full- and 4 half-adders." Becker, at 3. However, Becker does not teach or suggest "a controller configured to output, to said integer unit arithmetic circuit, a selection signal for selecting one of an integer unit arithmetic operation and finite field GF(2^m) based unit arithmetic operation," as required by amended claim 6.

Therefore, neither Glaser nor Becker, taken alone or in any reasonable combination, teaches or suggests all elements of Applicants' invention as recited in claim 6. Claim 6 is thus nonobvious over Glaser in view of Becker. Since claim 8

depends on claim 6, claim 8 is also nonobvious over Glaser in view of Becker. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 8.

Applicants also respectfully traverse the Examiner's rejection of claim 12 (dependent from claim 11) under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of New. As explained above, Dworkin fails to teach or suggest at least "an arithmetic unit module including a long product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression," as recited in amended claim 11.

New falls to cure Dworkin's deficiencies. New teaches method and apparatus for "summing the products of a predetermined number of successive pairs of numbers." New, abstract. However, New does not teach or suggest "an arithmetic unit module including a long product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression," as recited in amended claim 11.

Therefore, neither Dworkin nor New, taken alone or in any reasonable combination, teaches or suggests all elements of Applicants' invention as recited in claim 11. Claim 11 is thus nonobvious over Dworkin in view of New. Since claim 12 depends on claim 11, claim 12 is also nonobvious over Dworkin in view of New. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 12.

Applicants also respectfully traverse the Examiner's rejection of claim 13 (indirectly dependent from claim 11) under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of New, and further in view of Carroll. As discussed above, neither Dworkin nor New teaches or suggests "an arithmetic unit module including a long

product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression," as required by claim 11.

Carroll fails to cure Dworkin and New's deficiencies. Carroll teaches an asynchronous division apparatus "capable of sensing the completion of each addition operation to enable the system to proceed immediately to the operations subsequent thereto." Carroll, column 2, lines 20-24. However, Carroll fails to teach or suggest at least "an arithmetic unit module including a long product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression," as recited in amended claim 11.

Therefore, none of Dworkin, New, and Carroll, taken alone or in any reasonable combination, teaches or suggests all elements of Applicants' invention as recited in claim 11. Claim 11 is thus nonobvious over Dworkin in view of New and further in view of Carroll. Since claim 13 depends on claim 11, claim 13 is also nonobvious over Dworkin in view of New and further in view of Carroll. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 13.

Applicants also respectfully traverse the Examiner's rejection of claims 14 and 15 (indirectly dependent from claim 11) under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of New, further in view of Carroll, and further in view of Zook. As discussed above, neither Dworkin nor New teaches or suggests "an arithmetic unit module including a long product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression," as required by claim 11.

Zook, as well, fails to cure Dworkin, New, and Carroll's deficiencies. Zook teaches an inversion circuit which "determines an inverse B-1 of an m-bit finite field symbol B, the symbol B being expressed in a dual basis representation. The inversion circuit includes an iterative convolution circuit to which the symbol B is applied and which generates and stores electrical signals corresponding to an m-bit value." Zook, column 2, lines 40-46. However, Zook fails to teach or suggest at least "an arithmetic unit module including a long product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression," as recited in amended claim 11.

Therefore, none of Dworkin, New, Carroll, and Zook, taken alone or in any reasonable combination, teaches or suggests all elements of Applicants' invention as recited in claim 11. Claim 11 is thus nonobvious over Dworkin in view of New, further in view of Carroll, and further in view of Zook. Since claims 14 and 15 depend on claim 11, claims 14 and 15 are also nonobvious over Dworkin in view of New, further in view of Carroll, and further in view of Zook. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 14 and 15.

Regarding the Objections

Applicants have amended the title of the specification to be more descriptive according to the Examiner's suggestions. Applicants thank the Examiner for making suggestions and respectfully request withdrawal of the objection to the specification. Further, because amended claim 11 is allowable, as explained above, and claim 16 depends on amended claim 11, Applicants also request withdrawal the objection of claim 16 as dependent upon a rejected base claim.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: October 6, 2004

By: _____
Wenye Tan
Reg. No. 55,662